WSP ACCESS MISUSE/Security Procedure

212.1 PURPOSE

The purpose of this policy is to outline specific State requirements as it relates to WSP ACCESS misuse and violations.

212.2 DEFINITIONS

ACCESS: A Central Computerized Enforcement Service System.

FBI: Federal Bureau of Investigation

NICS: National Instant Background Check System.

TAC: Terminal Agency Coordinator. The point of contact within the agency who will serve as a liaison between the agency and the state ACCESS Auditors and Trainers.

WACIC: Washington Crime Information Center. State repository for law enforcement data.

WSP: Washington State Patrol

ORI: Originating Agency Identifier

Purpose Code: Reason for running the criminal history query.

QH: A query submitted through WSP ACCESS to determine the existence of a criminal record matching the inquiry. A positive criminal history response contains additional identifying data to associate the record with the person of the inquiry (height, weight, race, fingerprint and/or pattern classification, tattoos, etc.). The response also identifies the database(s) maintaining the criminal history information. With this information, the agency can decide whether to conduct a record request (QR).

QR: Request for a criminal history record from the FBI and/or the participating state(s) maintaining such record.

SID: State Identification Number. The number issued once a person is fingerprinted. This number will remain the same throughout a person's lifetime. The information from each fingerprint will be added to the original record (i.e. arrestees, dispositions, applicant information).

212.3 POLICY

(a) Use of the ACCESS System

(a) A Central Computerized Enforcement Service System (ACCESS) is a computer controlled communications system operated and maintained for all law enforcement and criminal justice agencies within the state. The Chief of the Washington State Patrol (WSP) administers all operating phases of the ACCESS System.

(b) The ACCESS System shall only be used for criminal justice purposes. The following rules and policies ensure proper and efficient use of the ACCESS

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

system. All terminal operators, including mobile data terminal users, must be certified at their appropriate role annually. All personnel will conform to these policies and rules. Any questions regarding these policies should be referred to the ACCESS Section.

All staff shall abide by the Policy and Procedures set forth by the FBI, NCIC, and ACCESS in the use of the State ACCESS System. All data received from the State System per the Policies and Procedures set forth under CJIS Security Policy in Code of Federal Regulation, Title 28, Part 20, Subparts A and C and by State statute in RCW 10.97 and Washington Administrative Code (WAC) 446-20.

212.4 TERMINAL AGENCY COORDINATOR

Terminal Agency Coordinator (TAC)

(a) The TAC is responsible for proper operator performance, strict adherence to regulations and prompt notification of CJIS violations to the ACCESS Section. Refer to the Introduction chapter of the ACCESS Operations Manual for further clarification of TAC responsibilities.

The Thurston County Sheriff's Office, Corrections Bureau must designate a Terminal Agency Coordinator (TAC) to act as the point of contact for the WSP and the Federal Bureau of Investigation (FBI).

The individual designated to function as a TAC will be responsible to ensure compliance with state and National Crime Information Center (NCIC) policies and regulations. The TAC must maintain a Level II training certification and attend TAC training once every three years.

The TAC shall participate in and ensure that all appropriate records be available during the triennial audit conducted by the ACCESS audit staff. Responsibility for proper operator performance, strict adherence to regulations, prompt notification of CJIS violations to the ACCESS Section, and subsequent training rests with the TAC.

212.5 USERS

All terminal users, including mobile data terminal users, must be certified at their appropriate level every two years. The Terminal Agency Coordinator (TAC) will monitor and track these certifications.

212.6 INFORMATION FROM ACCESS

Information from ACCESS and Dissemination

(a) All personnel who use, work on the connection to ACCESS, or have access to Criminal Justice Information (CJI) must observe all restrictions placed on the use or dissemination of information received through ACCESS. Policies contained within the ACCESS Operations Manual and other related manuals must be adhered to. Some

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

records may be public information; however, if the information is obtained through ACCESS it must only be used for criminal justice purposes. Those records that may be considered public would have to be released through a formal public disclosure request.

(b) Queries or messages not pertaining to law enforcement business (e.g., personal inquiries) are prohibited.

(c) Persons shall not use or provide any information obtained through the ACCESS system for private business or personal reasons.

Each user must observe all restrictions placed on the use or dissemination of information received through ACCESS. Policies contained within the ACCESS Manual, WACIC Manual, and other related manuals must be adhered to.

Persons shall not use any information obtained through the ACCESS system, including all Department of Licensing (DOL) and Department of Corrections (DOC) information, for private business or personal reasons or furnish any information so obtained to any other person for such use.

All Members of the Thurston County Sheriff's Office Corrections Bureau will ensure that:

(a) (a) All teletypes (printouts) will be kept from the public view.

(b) All criminal history information will be kept from public view.

(c) No persons outside of law enforcement will be left unattended where teletypes (printouts) are received or distributed.

(d) There will be no dissemination outside law enforcement.

(e) No NCIC will be conducted for personal use.

2. Any and all Criminal History and teletypes (printouts) will be placed:

3. In the inmate file; or In the shred bin.

4. The specifically designated shred bin will be located in a locked area and only accessible by certified ACCESS users.

1. All teletypes (printouts) will be placed in the shred bin at the end of each day when not retained for case use or dissemination.

2. Terminal Security

(a) (a) Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from unauthorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received. Federal and state laws protect the information provided by ACCESS.

212.7 SECURITY INCIDENT REPORTING

Security Incident Reporting

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

a. Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of Criminal Justice Information (CJI), agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

b. Thurston County Correctional Facility (TCCF) shall promptly report incident information to the ACCESS Section Manager using the ACCESS Violation Incident Report Form. The violation report can be found on the ACCESS website: http://www.wsp.wgov/_secured/access/resources.htm

c. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

d. The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

e. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

f. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

g. Mobile Devices-In addition to the requirements in Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office

h. Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
2. Device known to be locked, minimal duration of loss
3. Device lock state unknown, minimal duration of loss
4. Device lock state unknown, extended duration of loss
5. Device known to be unlocked, more than momentary duration of loss
6. Total loss of device
7. Device compromise
8. Device loss or compromise outside the United States

212.8 SYSTEM MISUSE

Violations of the rules, regulations, policies, or procedures developed by NCIC and adopted by the WSP or any other misuse or abuse of the ACCESS system may result in agency disciplinary measures and/or criminal prosecution.

(a) All allegations of ACCESS misuse must immediately be reported to the ACCESS Section Manager using the ACCESS Violation Incident Report Form. The violation report can be found on the ACCESS website: http://www.wsp.wa.gov/_secured/access/resources.htm

(b) If the allegations are founded, the investigating agency will choose the level of discipline.

(c) The WSP works in conjunction with the agency to impose additional sanctions, if warranted.

1. This may include but is not limited to, additional training, revocation of individual certification, or termination of system access to the department.

Copyright Lexipol, LLC 2025/01/02, All Rights Reserved.
Published with permission by Thurston County Sheriff's Office